I. PATENT ABSTRACTS OF JAPAN

(11)Publication number : **10-105516**
(43)Date of publication of application : **24.04.1998**

(51)Int.Cl. G06F 15/00
G06F 1/00
G06F 13/00
H04L 12/22
H04M 3/42
H04M 11/00

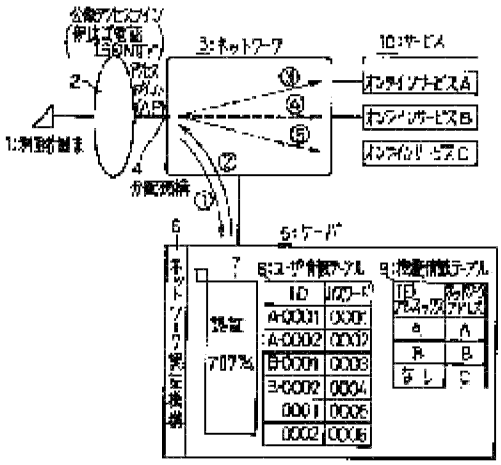
(21)Application number : **09-116899**
(22)Date of filing : **07.05.1997**

(71)Applicant : **FUJITSU LTD**
(72)Inventor : **SAWA HIROSHI**

(30)Priority
Priority number : **08122914** Priority date : **17.05.1996** Priority country : **JP**

(54) NETWORK AUTHENTICATION SYSTEM

(57)Abstract:



PROBLEM TO BE SOLVED: To improve the reliability of network security and to improve the security management of a service provider or to reduce the burden of security management by performing the security management at the entrance of a network by performing user authentication on the network when providing plural services from the same public access point, and connecting the access point while distributing it to the relevant service.

SOLUTION: A distributing mechanism 4 detects an incoming call from a user terminal 1 through a public line 2 to the access point of a certain network, transfers a user ID and a password to a network authentication mechanism 6 and connected any service designated out of plural services. While referring to a table 9 based on the user ID and the password transferred from this distributing mechanism 4, the relevant user ID and password are checked and in case of OK, the address of the relevant service is reported to the distributing mechanism 4.

CLAIMS

[Claim(s)]

[Claim 1] A network authentication system which attests two or more services, comprising:
A partition system linked to service which detected receipt to an access point of a network which has passed a public line from a user terminal, and transmitted a user ID and a password to a network authentication mechanism and as which it was specified of two or more services.
A network authentication mechanism which checks user ID concerned and a password with reference to a table, and notifies an address of applicable service to the time of O.K. to the above-mentioned partition system based on a user ID and a password which have been transmitted from this partition system.

[Claim 2] A network authentication system which attests two or more services, comprising:
A partition system linked to service which detected receipt to an access point of a network which has passed a public line from a user terminal, and transmitted a user ID and a password to an authentication server relay mechanism and as which it was specified of two or more services.
An authentication server relay mechanism which notifies an address which transmits to a server which takes charge of attestation of service of the user ID concerned with reference to a table about a user ID and a password which have been transmitted from the above-mentioned partition system, made it check, and had an answer of O.K. to the above-mentioned partition system.
A server which checks user ID concerned and a password with reference to a table, and notifies an address of applicable service to the time of O.K. to the above-mentioned authentication server relay mechanism based on a user ID and a password which have been transmitted from the above-mentioned authentication server relay mechanism.

[Claim 3] Claim 1 matching a part of above-mentioned user ID with the above-mentioned service, or the network authentication system according to claim 2.

[Claim 4] A partition system linked to service which detected receipt to an access point of a network which has passed a public line from a user terminal, and transmitted a user ID and a

password to a network authentication mechanism and as which it was specified of two or more services, Based on a user ID and a password which have been transmitted from this partition system, A storage which stored a program as which a network authentication mechanism which checks user ID concerned and a password with reference to a table, and notifies an address of applicable service to the time of O.K. to the above-mentioned partition system is operated.

[Translation done.]

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention]This invention relates to the network authentication system which attests two or more services.

[0002]

[Description of the Prior Art] When it connects with a network via a public line and service is provided conventionally, An access point (for example, telephone number for exclusive use) for exclusive use is provided for every service, and it connects with an applicable on-line service via a network from the access point concerned, and attests by the on-line service concerned (attestation of user ID and a password).

[0003] As shown in drawing 4, it distributes and connects for only every on-line service, and is made to attest at the entrance of the on-line service of a connection destination, when a commercial on line service entrepreneur provides two or more services from the same public access point individually, respectively.

[0004] When a commercial on line service entrepreneur provided two or more services from the same public access point, he attests by a certain on-line service, and was trying to connect with other on-line services by a gate way function, as shown in drawing 5.

[0005] The composition and operation of drawing 4 and drawing 5 are explained briefly below. Drawing 4 shows the explanatory view (the 1) of conventional technology. In drawing 4, a public access line is a public network for connecting with access point AP for receiving offer of an on-line service from a user terminal.

[0006] A network is a network of the entrepreneur who provides an on-line service. The on-line services A and B are servers etc. which provide on-line services, such as service of two or more kinds, for example, personal computer communications, and an Internet access service, and comprise an on-line service function, a user authentication function, etc.

[0007] An on-line service function provides various services for a user on-line. A user authentication function performs a user's user ID and attestation of a password.

[0008] Next, operation is explained.

** Telephone an access point from a user terminal.

The network which received the telephone by **** connects with the on-line service A applicable based on the specification from a user terminal, or the on-line service B.

[0009] The on-line service A connected by **** or the on-line service B performs attestation of user ID and a password, and provides service, respectively at the time of O.K.

[0010] Drawing 5 shows the explanatory view (the 2) of conventional technology. In drawing 5, a public access line is a public network for connecting with access point AP for receiving offer of an on-line service from a user terminal.

[0011] A network is a network of the entrepreneur who provides an on-line service. The on-line service A is a server etc. which provide an on-line service, and comprises a gate way function, an on-line service function, a user authentication function, etc. here.

[0012] A gate way function is transmitted to other applicable on-line services. An on-line service function provides various services for a user on-line.

[0013] A user authentication function performs a user's user ID and attestation of a password. Next, operation is explained.

[0014] ** Telephone an access point from a user terminal.

The network which received the telephone by **** connects with the one fixed on-line service A here.

[0015] The on-line service A connected by **** performs attestation of user ID and a password, and offer or a gate way function connects service to the on-line service of further others at the time of O.K.

[0016] other on-line services B connected by the gate way function by ****, for example, an on-line service, -- service -- offer -- or attestation of user ID and a password is performed further, and service is provided at the time of O.K.

[0017]

[Problem(s) to be Solved by the Invention] As mentioned above, under the composition of conventional drawing 4, (1) Are a different on-line service, and can share an access point, but. (2) In order to perform user authentication (attestation with user ID and a password) by the side which user authentication by the side of a network cannot be performed, and provides (3) on-line services, Could not attest at a network entrance, and security was missing, and there was a problem that it will be necessary to perform all the attestation and to secure security, in the on-line service which provides new service.

[0018] As mentioned above, under the composition of conventional drawing 5, (1) Are a different on-line service, and can share an access point, but. (2) The on-line service without (4) gate way functions which perform user authentication (attestation with user ID and a password) by the side which there is no user authentication by the side of a network, and provides (3) on-line services, Since service provision can be received only from the user of an on-line service who has a gate way function, cannot attest at a network entrance and security is missing, and. All the attestation was performed, it will be necessary to secure security and also and the service which can be received by the existence of a gate way function had a problem of producing restriction, in the on-line service which provides new service.

[0019] In order that this invention may solve these problems, when two or more services are provided from the same public access point, Distribute to the service which user authentication in a network is performed and corresponds, and it connects, A security management is performed at a network entrance and it aims at improving the reliability of network security, raising security management of a purveyor of service, or easing the burden of a security management.

[0020]

[Means for Solving the Problem] With reference to drawing 1 and drawing 2, The means for solving a technical problem is explained. In drawing 1 and drawing 2, the user terminal 1 enters a user ID and a password, and uses service.

[0021] the partition system 4 detecting receipt from the user terminal 1, and connecting a user ID and a password to the service 10 as which it was specified of two or more services [**** /

transmitting to the network authentication mechanism 6 or the authentication server relay mechanism 12] **** -- etc. -- it carries out.

[0022] The service 10 provides various services. Next, operation is explained. The partition system 4 of the network 3 detects receipt to an access point from the user terminal 1 via a public line, Transmit a user ID and a password to the network authentication mechanism 6, the network authentication mechanism 6 checks with reference to a table based on a user ID and a password, and an address of service to the time of O.K. is notified to the partition system 4, It connects with an address with which the partition system 4 was specified, and he connects the applicable service 10 with the user terminal 1, and is trying for the user terminal 1 concerned to receive service provision from the service 10.

[0023] The partition system 4 of the network 3 detects receipt to an access point from the user terminal 1 via a public line, Transmit a user ID and a password to the authentication server relay mechanism 12, and the authentication server relay mechanism 12 transmits to a server which takes charge of attestation of service of the user ID concerned with reference to a table, With reference to a table, check user ID concerned and a password based on a user ID and a password with which a server has been transmitted, and an address of service to the time of O.K. is notified to the partition system 4 via an authentication server relay mechanism, It connects with an address with which the partition system 4 was specified, and he connects the applicable service 10 with the user terminal 1, and is trying for the user terminal 1 concerned to receive service provision from the service 10.

[0024] Under the present circumstances, he is trying to match a part of user ID with the service 10. Therefore, by distributing to the service 10 which user authentication in a network is performed and corresponds, connecting, and performing a security management at a network entrance, when plurality carries out service provision from the same public access point, It becomes possible to improve the reliability of network security, to raise security management of a purveyor of service, or to ease a burden of a security management.

[0025]

[Embodiment of the Invention] Next, an embodiment of the invention and operation are explained to details one by one using drawing 3 from drawing 1. Here, it reads from the storage besides a graphic display of the program as which each mechanism of drawing 1 is operated, and

on the main memory (server etc.) of an applicable computer system, loading is carried out, it starts, and various processing explained below is performed.

[0026] Drawing 1 shows 1 example lineblock diagram of this invention. In drawing 1, the user terminal 1 is for a user's operating it, entering a user ID and a password, connecting with the service 10, and receiving offer of various services.

[0027] It connects with the arbitrary access points of the network 3, and the public access line 2 is a telephone line, an ISDN circuit, etc. which are public lines. Call origination is carried out to the specific telephone number of access point AP using this public access line 2, and he connects with the service 10, and is trying for the user terminal 1 to receive offer of various services.

[0028] The network 3 is a network by the side of a purveyor of service which connects from the specific access point of a public access line, and has the partition system 4 etc. here.

[0029] The partition system 4 receives the arrival from a public access line to the access point of the network 3, or, connecting the call which carried out receipt of the user ID and password which were received from the user terminal 1 to the service 10 of the address which transmitted to the network authentication mechanism 6, or was notified from the network authentication mechanism 6 **** -- etc. -- it carries out.

[0030] The server 5 performs various processing and comprises the network authentication mechanism 6 etc. here. The network authentication mechanism 6 attests based on a user ID and a password, and comprises the authentication program 7, a User Information initial entry table 8 and 9, etc. here.

[0031] that the authentication program 7 takes out the address of the service 10 which attests with reference to the User Information table 8, and performs service provision about a user ID and a password at the time of O.K. from the initial entry table 9 **** -- etc. -- it carries out.

[0032] The User Information table 8 registers a user ID and a password. The initial entry table 9 registers the address of the service 10 which provides service for a user.

[0033] Next, operation is explained. In drawing 1, ** performs a user authentication demand (a user ID / pass-word-authentication demand). When the partition system 4 carries out receipt of this to access point AP by the public access line 2 from the user terminal 1, it transmits the user ID and password which have been transmitted to the server 5.

[0034] ** Perform a user authentication reply (a user ID / password check reply, and a connection network address reply). The authentication program 7 which constitutes the network authentication mechanism 6 of the server 5 attests with reference to the User Information table 8 about the user ID and password with which this received transmission by ** (it is a deed about the check of whether a user ID and a password are in agreement), With reference to the initial entry table 9, the network address (address of the service 10 beforehand defined by the prefix) corresponding to the prefix of a user ID is taken out at the time of O.K., and it notifies to the partition system 4.

[0035] ** It is connection in case ID prefix is A. This connects to the on-line service A of the network address A the call which carried out receipt to the access point, when the network address where the partition system 4 was notified by ** is A.

[0036] Similarly, ** and ** are connection in case ID prefix is B or C. This connects to the on-line service B of the network address B the call which carried out receipt to the access point at the on-line service C of connection or the network address C, when the network address where the partition system 4 was notified by ** is B or C.

[0037] By the above, when network access point AP has receipt via a public access line from the user terminal 1, By attesting by transmitting the user ID and password which have been transmitted to the network authentication mechanism 6, connecting with the applicable on-line service notified at the time of O.K., and providing service, It can attest at a network entrance, and can make network security into high-reliability, and. It distributes to the service 10 applicable after performing network authentication, and connects, and it attests further with the service 10 concerned, and it becomes possible to raise security, or to omit attestation at the entrance of the service 10 concerned, since attestation has already been carried out at the network entrance.

[0038] Drawing 2 shows other example lineblock diagrams of this invention. Here, since the user terminal 1, the public access line 2, the network 3, and the service 10 are the same as the thing of the same number of drawing 1, explanation is omitted.

[0039] In drawing 2, the server 11 performs various processing and comprises the authentication server relay mechanism 12 etc. here. The authentication server relay mechanism 12 transmits the user ID and password which have been transmitted from the partition system 4 of the network 3 to the applicable network authentication mechanism 16, or, notifying the network address of the

connection destination notified from the network authentication mechanism 16 to the partition system 4 **** -- etc. -- it carries out and comprises authentication server selection / the relay program 13, the server correspondence table 14, etc.

[0040] notifying authentication server selection / relay program 13 to the partition system 4, when take out an authentication server based on the prefix of a user ID, and a user ID and a password are transmitted to this server or an authentication result is received with reference to the server correspondence table 14 **** -- etc. -- it carries out.

[0041] The server correspondence table 14 registers beforehand the authentication server which attests by matching with PUREIKKUSU of a user ID. The server 15 attests based on a user ID and a password, and comprises the network authentication mechanism 16 etc. here.

[0042] The network authentication mechanism 16 attests based on a user ID and a password, and comprises the authentication program 17, a User Information table 18, the address table 19, etc. here. Thus, by having established the network authentication mechanism 16 every service 10, The route which attests at the entrance of the network 3 of the invention in this application which manages a user ID and a password unitary every service 10, and is shown in drawing 2, When performing attestation with the conventional user IDs and passwords for exclusive use to an access point from the user terminal 1 for every service 10 in parallel, [other than drawing 2] The things (a user ID and the new registration of a password, correction, deletion, etc.) for which a user ID and a password are easily managed unitary for every service become possible.

[0043] that the authentication program 17 takes out the address of the service 10 which attests with reference to the User Information table 18, and performs service provision about a user ID and a password at the time of O.K. from the address table 19 **** -- etc. -- it carries out.

[0044] The User Information table 18 registers a user ID and a password. The address table 19 registers the connection network address of the service 10 which provides service for a user.

[0045] Next, operation is explained. In drawing 2, ** performs a user authentication demand (a user ID / pass-word-authentication demand). When the partition system 4 carries out receipt of this to access point AP by the public access line 2 from the user terminal 1, it transmits the user ID and password which have been transmitted server 11.

[0046] ** Choose an authentication server by ID prefix and relay a user authentication demand. This takes out the authentication server whose authentication server selection / relay program 13 which constitutes the authentication server relay mechanism 12 of the server 11 correspond with the prefix of a user ID with reference to the server correspondence table 14 about the user ID and password which received transmission by **, A user authentication demand (a user ID / password-authentication demand) is relayed.

[0047] ** Perform a user authentication reply (a user ID / password check, and a connection network address reply). The authentication program 17 which constitutes the network authentication mechanism 16 of the server 15 attests with reference to the User Information table 18 about the user ID and password with which this received relay by ** (it is a deed about the check of whether a user ID and a password are in agreement), With reference to the address table 19, a connection network address is taken out at the time of O.K., and it notifies to the authentication server relay mechanism 12.

[0048] ** Relay the user authentication reply from each server to the partition system 4 of an access point. This notifies the user authentication reply (reply of the connection network address at the time of O.K.) from each server to the partition system 4 by **.

[0049] ** It is connection in case ID prefix is AAA. This connects to the on-line service A of network address A.A.A.A. the call which carried out receipt to the access point, when the connection network address where the partition system 4 was notified by ** is A.A.A.A.

[0050] Similarly, ** and ** are connection in case ID prefix is BBB or CCC. When B.B.B.B. or a connection network address is C.C.C.C., the connection network address where the partition system 4 was notified by ** this, The call which carried out receipt to the access point is connected to the on-line service B of network address B.B.B.B. at the on-line service C of connection or network address C.C.C.C.

[0051] By the above, when network access point AP has receipt via a public access line from the user terminal 1, The user ID and the PASSU word which has been transmitted are transmitted to the authentication server relay mechanism 12, By attesting by hooking up to the applicable network authentication mechanism 16, connecting with the applicable on-line service notified at the time of O.K., and providing service, It can attest at a network entrance, and can make network security into high-reliability, and. Distribute to the service 10 applicable after

performing network authentication, and it connects, Become possible to attest further with the service 10 concerned, to raise security, or to omit attestation at the entrance of the service 10 concerned, since attestation has already been carried out at the network entrance, and. The things (a user ID and the new registration of a password, correction, deletion, etc.) which the network authentication mechanism 16 is established every service 10, and are managed unitary every service 10 by being a line in attestation of a user ID and a password become possible.

[0052] Next, operation of the composition of drawing 2 is explained in detail using drawing 3. Drawing 3 shows the explanatory view of this invention of operation. Here, the server S expresses the server 11 of drawing 2, the server SAAA, the server SBBB, and the server SCCC express the server 15 of drawing 2, and an access point expresses the access point of drawing 2.

[0053] In drawing 3, S1 receives ID/PW. As for this, the authentication server relay mechanism 12 of the server 11 of drawing 2 receives the user ID and password from the user terminal 1.

[0054] S2 identifies the head of three characters and passes ID/PW to an applicable server. This identifies three characters "AAA" of the head which is a prefix of discernment, for example, a user ID, about the head of three characters of the user ID which received by S1, An authentication server "SAAA" is taken out with reference to the server correspondence table 14 of drawing 2, and a user ID and a password are passed to this authentication server "SAAA." And S3 thru/or S9 are performed in this example.

[0055] S3 performs attestation for on-line service A (authentication check corresponding to ID information). Since this was proved by S2 that it is user ID prefix =AAA and the user ID and the password were passed to the server SAAA, the authentication program 17 of drawing 2 confirms whether the user ID and the password are registered with reference to the User Information table 18. In O.K., a network address (connection network address taken out from the address table 19 of drawing 2) is returned to an access point (partition system 4) by S4, A call is connected to the on-line service A by S6, and the user terminal 1 connects with the on-line service A, and receives service provision. On the other hand, in the case of NG, an improper notice is returned by S7, the improper notice which received by S8 is returned to an access point, and the partition system 4 cuts a call by S9.

[0056] When similarly it is proved by S2 that they are user ID prefix =BBB or user ID prefix =CCC, It connects with the on-line service B or the on-line service C by S13 thru/or S19, or S23

thru/or S29 at the time of the attestation O.K., or, on the other hand, cuts at the time of attestation NG.

[0057]

[Effect of the Invention]As explained above, when plurality carries out service provision from the same public access point according to this invention, Since the composition which distributes to the service 10 which user authentication in a network is performed and corresponds, connects, and performs a security management at a network entrance is adopted, The reliability of network security is improved, security management of a purveyor of service can be raised, or the burden of a security management can be eased.

[Translation done.]

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1]It is 1 example lineblock diagram of this invention.

[Drawing 2]They are other example lineblock diagrams of this invention.

[Drawing 3]It is an explanatory view of this invention of operation.

[Drawing 4]It is an explanatory view (the 1) of conventional technology.

[Drawing 5]It is an explanatory view (the 2) of conventional technology.

[Description of Notations]

1: User terminal

2: Public access line (public network)

3: Network

4: Partition system

5, 11, 15: Server

6, 16: Network authentication mechanism

7, 17: Authentication program

8, 18: User Information table

9: Initial entry table

10: Service

12: Authentication server relay mechanism

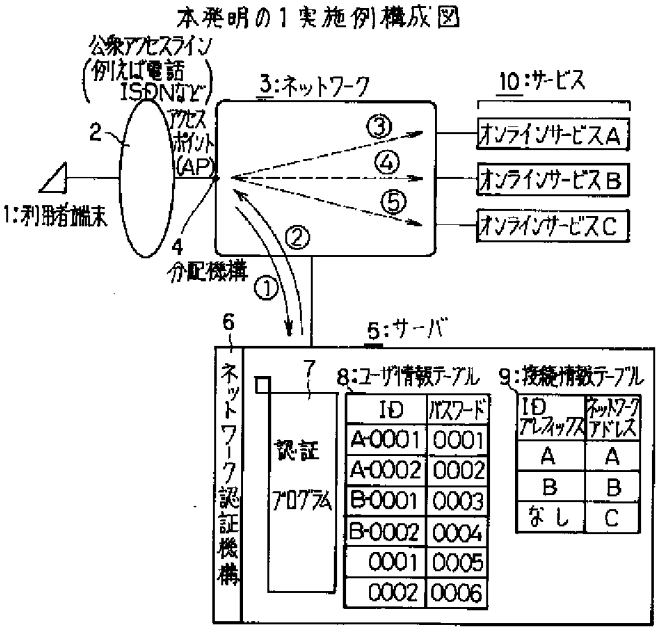
13: Authentication server selection / relay program

14: Server correspondence table

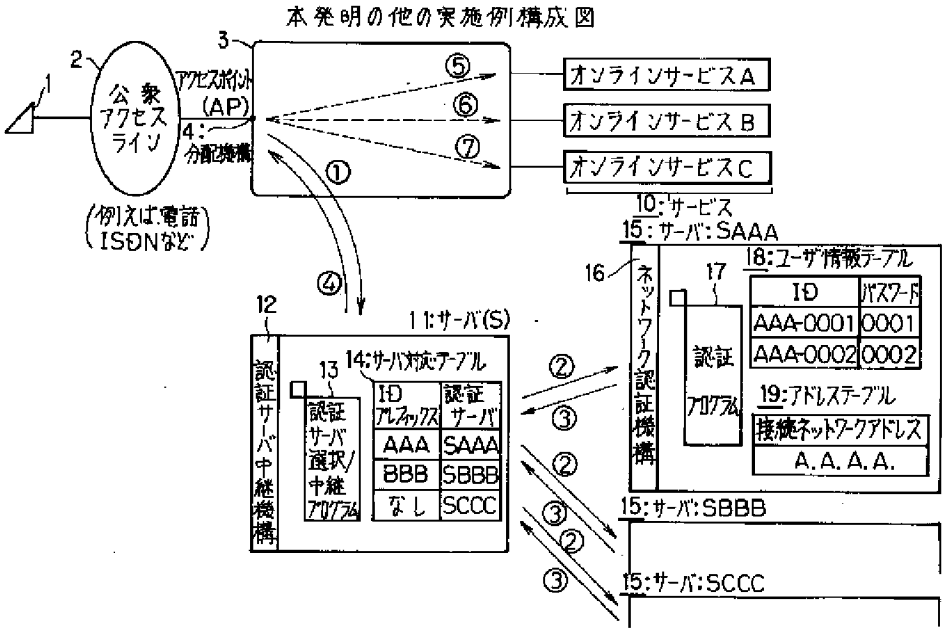
19: Address table

DRAWINGS

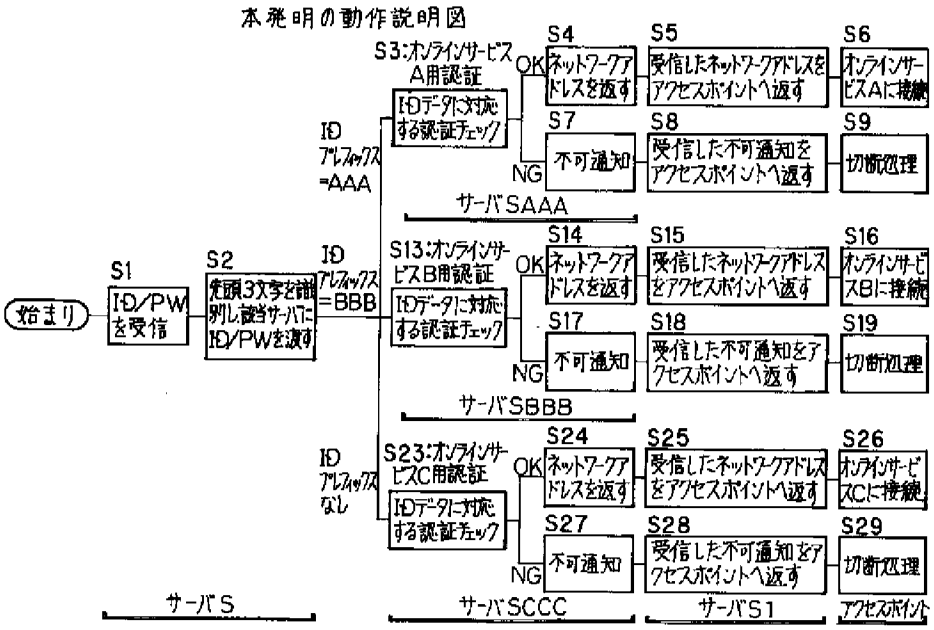
[Drawing 1]



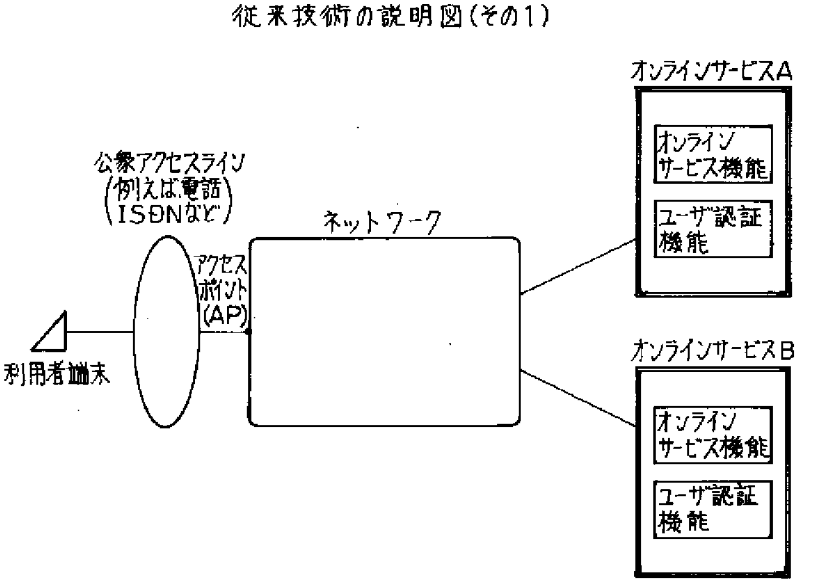
[Drawing 2]



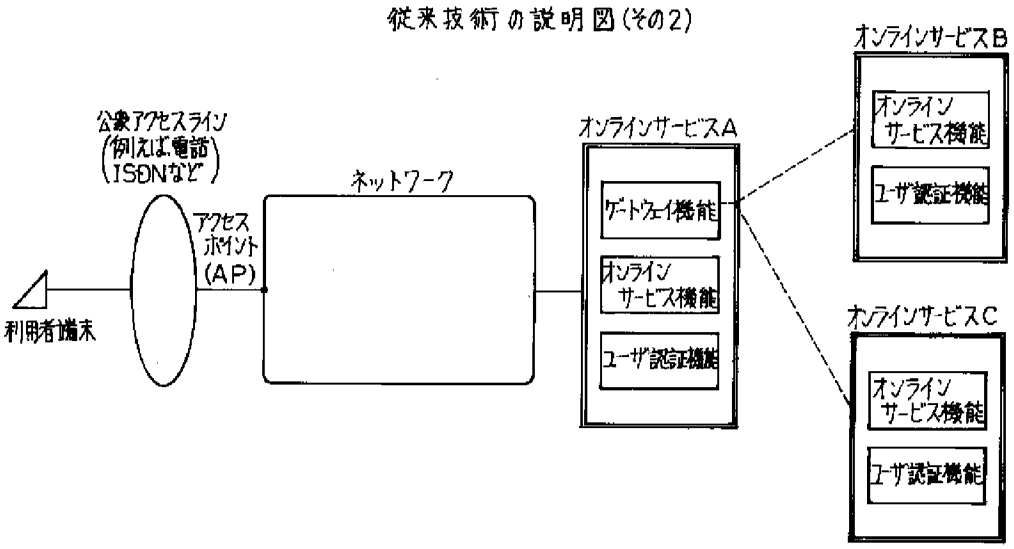
[Drawing 3]



[Drawing 4]



[Drawing 5]



[Translation done.]

8582043
021810